Computer Science Depa

TECHNICAL REPORT

On the Decidability of Presburger Arithmetic with Homogeneous Exponentiation

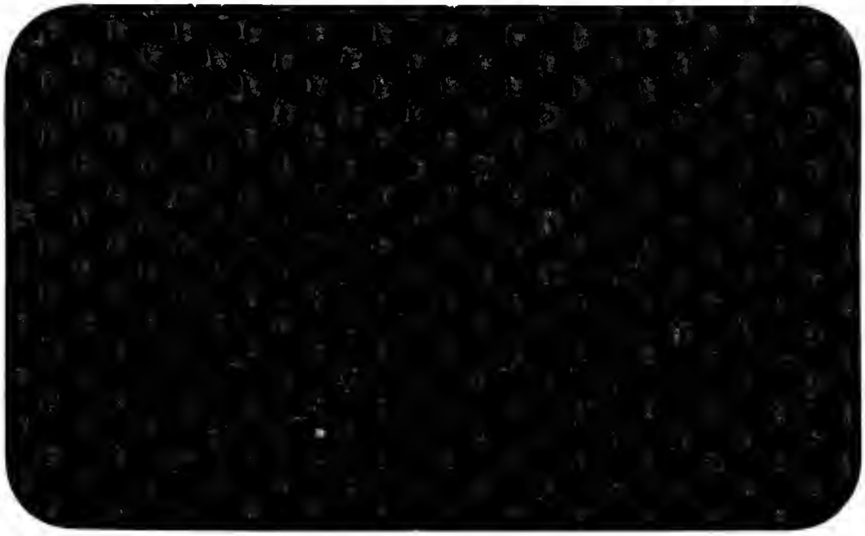
D. Cantone

Technical Report 450

May 1989

NEW YORK UNIVERSITY

Department of Computer Science
Courant Institute of Mathematical Sciences
251 MERCER STREET, NEW YORK, N.Y. 10012



On the Decidability of Presburger Arithmetic with Homogeneous Exponentiation

D. Cantone

Technical Report 450

May 1989

On the decidability of Presburger arithmetic with homogeneous exponentiation *

D. CANTONE
Courant Institute, New York University
251 Mercer St., New York, New York 10012; and
Mathematics Dept., University of Catania
Viale A. Doria, 6 A, 95125 Catania, ITALY.

1 Introduction

One of the basic problems of mathematical logic and theoretical computer science is to find as a tight boundary as possible between the decidable and the undecidable. Many advances in this direction have recently been made for some fragments of set theory (see for example [CFO,BFOS81,PP88,CCP89,CC89]).

In this paper we show that Presburger arithmetic (which is well known to be decidable; see [Pre29,End72]) can be extended with "homogeneous" exponentiation without disrupting decidability. We will be more specific below on what we mean by homogeneous exponentiation (in short: h.e.).

It is known that the most interesting and expressive theories are intractable, when decidable. This is, for instance, the case for every (logical) theory which can express the propositional calculus. In fact, from the result of Fisher and Rabin (cf. [FR74]), it follows that Presburger arithmetic has a nondeterministic time lower bound of $2^{2^{cn}}$. Obviously, the same result also holds when h.e. is admitted.

Nevertheless, even intractable decision procedures are amenable of practical utilizations for small fragments of their domain of application. For instance, despite of the super-exponential lower bound cited above, unquantified Presburger arithmetic is $\mathcal{NP}$-complete (see [Pap81]). This fact has been generalized in [Sho79] and [SJ80], which give nondeterministic polynomial time decision procedures for unquantified Presburger formulae extended respectively with uninterpreted predicate and function symbols and with array constructs. Likewise, it turns out that unquantified Presburger arithmetic with h.e. is $\mathcal{NP}$-complete.

In the following section we will give some basic definitions. Then, in Section 3 we will show how to eliminate the exponentiation operator from Presburger formulae with h.e.. For ease of exposition, the reduction provided is not optimal. Section 4 will hint the changes needed to

*This work has been partially supported by ENI and ENIDATA within the AXL project.

prove the $\mathcal{NP}$-completeness of the unquantified theory. Section 5 discusses some applications. The paper is then concluded with some conjectures.

2 Definitions and examples

Presburger arithmetic (PA) is the first-order theory of natural numbers $\mathcal{N}$ with addition $+$ and equality $=$. A decision procedure for PA has been first given in 1929 (cf. [Pre29]). Since then, several improvements both in space and time complexity have been made (see [Coo71,Coo72,RD78,Opp78,Sca84]). Some authors have also considered extensions of PA with functional and predicative constructs, such as the array operator and the predicate *Perm* (see [SJ80,Sho79]), but only for unquantified formulae.

It is well known that arithmetic, i.e. the first order theory of natural numbers with addition and multiplication, is undecidable (see [Chu36]). Therefore, any extension of PA which is powerful enough to express integer multiplication is undecidable. For instance, PA with array constructs is undecidable (cf. [SJ80]) as well as PA extended with a single monadic predicate letter (cf. [Dow72]). From the unsolvability of Hilbert's tenth problem (cf. [Mat70] and [Dav73]), it follows that even the satisfiability problem for the class of purely existential formulae of arithmetic cannot be decided. This last result implies that the class of existentially quantified formulae of PA extended by any operation which allows to instantiate multiplication in a purely existential fashion is also undecidable. Thus, for instance, one has that the satisfiability problem for the quantifier-free extensions of PA with any of the following operations is undecidable

- $\mathit{square}(x)$, i.e. the function x^2,
- $\mathit{power\_n}(x)$, i.e. the function x^n, for any fixed natural number n,
- $\mathit{exp}(x, y)$, i.e. the function x^y.

To show that the literal $z = x \cdot y$ can be expressed by means of the function $\mathit{square}(x)$, it is enough to consider the formula

$$z + z + \mathit{square}(x) + \mathit{square}(y) = \mathit{square}(x + y)\ .$$

Similar formulae can also be written when the function $\mathit{power\_n}(x)$ is admitted in place of $\mathit{square}(x)$, for $n \geq 3$. Finally, since $\mathit{square}(x) \equiv \mathit{exp}(x, 2)$, the unquantified subtheory of PA + *exp* is undecidable as well.

In this paper we consider a significantly restricted subclass of formulae of additive arithmetic with exponentiation, whose decision problem can be reduced to that of PA. It is obtained from the theory PA + *exp* by imposing certain syntactical constraints on matrices of quantified formulae, no constraint being put on quantifiers. We will refer to such formulae as *E-homogeneous* Presburger formulae and we will denote their class by $\mathrm{PAE_{Hom}}$. So, the language of $\mathrm{PAE_{Hom}}$ will have the operators $+$ and *exp* and the relation symbols $=$ and $<$ (we include the symbol $<$ in the language because otherwise the relation $t < u$, with t and u containing *exp*, would not be immediately expressible using $\mathrm{PAE_{Hom}}$-formulae).

For simplicity, in the following we will write x^y in place of $\mathit{exp}(x, y)$.

DEFINITION 2.1 *Let $T = \{t_i : i = 1, \ldots, n\}$ be a set of terms in the language $+$, exp. Then T is said to be E-*homogeneous *if either*

(a) each $t_i \in T$ is a purely additive term of Presburger arithmetic, i.e. each t_i is exponentiation free; or

(b) all terms $t_1, \ldots, t_n$ are of the form $t^{u_1}, \ldots, t^{u_n}$, for some E-homogeneous term t, and some E-homogeneous set of terms $\{u_1, \ldots, u_n\}$.

A term t is E-homogeneous if t is of the form $t_1 + \cdots + t_n$, with $n \geq 1$, and the set $\{t_1, \ldots, t_n\}$ is E-homogeneous. □

DEFINITION 2.2 *An atomic formula of type $t = u$ or $t < u$ is E-homogeneous if the term $t + u$ is E-homogeneous.*

A formula is E-homogeneous if all its atoms are E-homogeneous.

The class of E-homogeneous formulae is denoted by $\mathrm{PAE}_{\mathrm{Hom}}$. □

Examples.

- The set of terms

$$T = \left\{ \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z_1}} , \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z_4+z_5}} , \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z}} \right\}$$

  is E-homogeneous, whereas

$$T \cup \left\{ \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{{z_1}^{z_2}}} \right\}$$

  is not E-homogeneous.

- The term $x^{y^{z_1}+y^{z_2}}$ is E-homogeneous, whereas the terms $x^{y^{z_1}+z^{z_2}}$ and $x + x^y$ are not E-homogeneous.

- The formula

$$(\forall x)(\exists y)(\forall z_1, z_2, z_3, z_4, z_5)(\exists z) \left(\left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z_1}} + \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z_4+z_5}} = \left(x^{y^{z_1}+y^{z_2}}\right)^{{z_3}^{z}} \right)$$

  is E-homogeneous.

In the following section we will show how to effectively reduce any $\mathrm{PAE}_{\mathrm{Hom}}$-formula to a logically equivalent PA-formula, thus proving the decidability of the class $\mathrm{PAE}_{\mathrm{Hom}}$.

3 The main result

In this section we will show how to eliminate exponentiation from E-homogeneous atomic formulae. Specifically, we will provide transformation rules that given any E-homogeneous atomic formula $\varphi(x_1, \ldots, x_n)$ will produce another E-homogeneous quantifier-free formula $\psi(x_1, \ldots, x_n)$ (not necessarily atomic) such that

(i) each atom in $\psi(x_1, \ldots, x_n)$ contains less occurrences of the exponentiation operator than $\varphi(x_1, \ldots, x_n)$, and

(ii) the formula

$$(\forall x_1) \cdots (\forall x_n)(\varphi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n))$$

is valid.

Therefore, by repeatedly applying the transformations to be described below, one can reduce the decision problem for $\mathrm{PAE}_{\mathrm{Hom}}$ to that of PA.

For simplification purposes, we will make the convention that

$$0^0 = 0\ .$$

Let us begin by first considering E-homogeneous atomic formulae of type

$$t^{u_1} + t^{u_2} + \ldots + t^{u_n} = t^{v_1} + t^{v_2} + \ldots + t^{v_m}\ . \tag{1}$$

Clearly, (1) is equivalent to the disjunction of the following two formulae

$$t \leq 1 \quad \wedge \quad t^{u_1} + t^{u_2} + \ldots + t^{u_n} = t^{v_1} + t^{v_2} + \ldots + t^{v_m} \tag{2}$$

$$t \geq 2 \quad \wedge \quad t^{u_1} + t^{u_2} + \ldots + t^{u_n} = t^{v_1} + t^{v_2} + \ldots + t^{v_m}\ . \tag{3}$$

It is immediate to see that (2) is equivalent to

$$t = 0 \vee (t = 1 \wedge m = n)\ . \tag{4}$$

REMARK 3.1 Notice that (4) contains atoms of type $t = k$, with t E-homogeneous and k an integer constant, which are not E-homogeneous according to Definition 2.2. Nevertheless, below we will show how to eliminate exponentiation from such atoms and also from atoms of the form $t = u + k$, with t, u E-homogeneous and k an integer constant. □

We will use the notation $I_n = \{1, \ldots, n\}$. Also, $A \subseteq B$ [resp. $A \subset B$] will be used throughout to denote that A is a subset of B [resp. A is a proper subset of B].

To reduce formula (3), we will consider separately the cases in which $n = m = 1$, $n > m = 1$, and $n, m > 1$ (case $m > n = 1$ is completely identical to case $n > m = 1$), where n and m are respectively the number of addends in the left- and right-hand sides of (1).

Case $n = m = 1$. In this case (3) becomes $t \geq 2 \wedge t^{u_1} = t^{v_1}$ which is clearly equivalent to

$$t \geq 2 \wedge u_1 = v_1\ . \tag{5}$$

Case $n > m = 1$. In this case (3) becomes

$$t \geq 2 \wedge t^{u_1} + t^{u_2} + \ldots + t^{u_n} = t^{v_1} \,. \tag{6}$$

We claim that (6) is equivalent to

$$\bigvee_{k=2}^{n} \left(t = k \wedge \left(\bigvee_{\substack{A \subset I_n, h \in I_n, i_0 \in I_n \\ |A| = k^h}} \left(\bigwedge_{a \in A} u_{i_0} = u_a + h \wedge t^{u_{i_0}} + \sum_{i \in I_n \setminus A} t^{u_i} = t^{v_1} \right) \right. \right.$$
$$\left. \left. \vee \bigvee_{\substack{h \in I_n \\ k^h = n}} \left(\bigwedge_{i \in I_n} v_1 = u_i + h \right) \right) \right) \,. \tag{7}$$

It is immediate to see that (7) implies (6). To show the converse, we proceed as follows. Let $p \geq 2$, $q_1, \ldots, q_n, r_1 \geq 0$ ($n \geq 2$) be natural numbers such that $\sum_{i \in I_n} p^{q_i} = p^{r_1}$. Then $p \leq n$. In fact, if $p > n$, by putting $\overline{q} = \max\{q_1, \ldots, q_n\}$, we would have $\sum_{i \in I_n} p^{q_i} \leq n \cdot p^{\overline{q}} < p^{r_1}$, a contradiction.

If $q_1 = q_2 = \ldots = q_n$, then $n \cdot p^{q_1} = p^{r_1}$, so that $\log_p n$ is an integer, and $r_1 = q_i + \log_p n$, $i \in I_n$. On the other hand, if $q_i \neq q_j$ for some $i, j \in I_n$, then by putting $q' = \min\{q_i \ : \ i \in I_n\}$ and $q_{i_0} = \min\{q_i \ : \ i \in I_n \text{ and } q_i \neq q'\}$, it follows that

$$|\{i \in I_n \ : \ q_i = q'\}| \geq p^{q_{i_0} - q'} \,.$$

Thus, (7) can be satisfied by p, q_i, r_1 by taking $A \subseteq \overline{A}$ such that $|A| = p^h$, with $h = q_{i_0} - q'$.

Below we will show how to deal with atoms of type $v_1 = u_i + h$.

Case $n, m > 1$. Let us denote by $\mathcal{A}$ the formula

$$\bigvee_{\substack{A \subseteq I_n \\ j_0 \in I_m}} \left(\sum_{a \in A} t^{u_a} = t^{v_{j_0}} \wedge \sum_{i \in I_n \setminus A} t^{u_i} = \sum_{\substack{j \in I_m \\ j \neq j_0}} t^{v_j} \right) \vee \bigvee_{\substack{B \subseteq I_m \\ i_0 \in I_n}} \left(t^{u_{i_0}} = \sum_{b \in B} t^{v_b} \wedge \sum_{\substack{i \in I_n \\ i \neq i_0}} t^{u_i} = \sum_{j \in I_m \setminus B} t^{v_j} \right) \,.$$

Then in this case (3) is equivalent to

$$t \geq 2 \wedge \mathcal{A} \,. \tag{8}$$

Again, it is plain that (8) implies (3). To show the converse, we use the following elementary lemma.

LEMMA 3.2 *Let $p \geq 2$ and let $0 \leq q_1, \ldots, q_n \leq r$ such that $\sum_{i \in I_n} p^{q_i} > p^r$. Then, $\sum_{a \in A} p^{q_a} = p^r$, for some $A \subset I_n$.*

Proof. Suppose by way of contradiction that the lemma is false. Let $\overline{A} \subseteq I_n$ be such that $\sum_{a \in \overline{A}} p^{q_a} > p^r$ and $\sum_{\substack{a \in \overline{A} \\ a \neq a_0}} p^{q_a} < p^r$, for all $a_0 \in \overline{A}$. Let $q_{a^*} = \min\{q_a \ : \ a \in \overline{A}\}$. Then

$p^{q_{a^*}} \mid p^r - \sum_{\substack{a\in\overline{A}\\ a\neq a^*}} p^{q_a}$, so that $p^r - \sum_{\substack{a\in\overline{A}\\ a\neq a^*}} p^{q_a} \geq p^{q_{a^*}}$, contradicting the assumption $\sum_{a\in\overline{A}} p^{q_a} > p^r$. ■

Now, assume that $\sum_{i\in I_n} p^{q_i} = \sum_{j\in I_m} p^{r_j}$, for $p \geq 2$, and $q_i, r_j \geq 0$, with $i \in I_n$ and $j \in I_m$ $(n, m > 1)$. Let $q' = \min\{q_i \ : \ i \in I_n\}$ and $r' = \min\{r_j \ : \ j \in I_m\}$. If $q' = r'$, (8) follows immediately. So assume that $q' < r'$. Let $\overline{A} = \{i \ : \ q_i < r'\}$. Then $p^{r'} \mid \sum_{i\in\overline{A}} p^{q_i}$, so that $\sum_{i\in\overline{A}} p^{q_i} \geq p^{r'}$. Then, Lemma 3.2 implies that (8) is satisfied by p, q_i, r_j. The case $q' > r'$ is completely analogous to the preceding.

Next we consider atomic formulae of type

$$t^{u_1} + t^{u_2} + \ldots + t^{u_n} < t^{v_1} + t^{v_2} + \ldots + t^{v_m} \ . \tag{9}$$

These are equivalent to the disjunction of the following two formulae

$$t \leq 1 \quad \wedge \quad t^{u_1} + t^{u_2} + \ldots + t^{u_n} < t^{v_1} + t^{v_2} + \ldots + t^{v_m} \tag{10}$$

$$t \geq 2 \quad \wedge \quad t^{u_1} + t^{u_2} + \ldots + t^{u_n} < t^{v_1} + t^{v_2} + \ldots + t^{v_m} \ . \tag{11}$$

Plainly, (10) is equivalent to

$$t = 1 \wedge n < m \ .$$

Formula (11) will be dealt with by considering separately the cases $n = m = 1$, $n > m = 1$, and $m > 1$.

Case $n = m = 1$. In this case (11) becomes $t \geq 2 \wedge t^{u_1} < t^{v_1}$ which is clearly equivalent to

$$t \geq 2 \wedge u_1 < v_1 \ . \tag{12}$$

Case $n > m = 1$. In this case (11) becomes

$$t \geq 2 \wedge t^{u_1} + t^{u_2} + \ldots + t^{u_n} < t^{v_1} \ . \tag{13}$$

Let us show that (13) is equivalent to

$$t \geq 2 \wedge \bigwedge_{i\in I_n} u_i < v_1 \wedge \bigwedge_{A\subseteq I_n} \sum_{a\in A} t^{u_a} \neq t^{v_1} \ . \tag{14}$$

Plainly, (14) implies (13). To prove the converse implication, let $n, p \geq 2$, $r_1 \geq 0$, $q_i \geq 0$, with $i \in I_n$, be natural numbers satisfying (13), i.e. such that $\sum_{i\in I_n} p^{q_i} < p^{r_1}$. Since $p^{q_i} < p^{r_1}$, $i \in I_n$, by Lemma 3.2 we have $\sum_{a\in A} p^{q_a} < p^{r_1}$, for all $A \subseteq I_n$. This in turn implies $\sum_{a\in A} p^{q_a} \neq p^{r_1}$, i.e. (14) is satisfied by p, q_i, r_1, proving that (14) is implied by (13).

Case $m > 1$. Let us denote by $\mathcal{B}$ the formula

$$\bigvee_{\substack{A\subseteq I_n\\ j_0\in I_m}} \left(\sum_{a\in A} t^{u_a} = t^{v_{j_0}} \wedge \sum_{i\in I_n\setminus A} t^{u_i} < \sum_{\substack{j\in I_m\\ j\neq j_0}} t^{v_j} \right) \vee \bigvee_{\substack{B\subseteq I_m\\ i_0\in I_n}} \left(t^{u_{i_0}} = \sum_{b\in B} t^{v_b} \wedge \sum_{\substack{i\in I_n\\ i\neq i_0}} t^{u_i} < \sum_{j\in I_m\setminus B} t^{v_j} \right) \ .$$

Then (11) is equivalent to

$$t \geq 2 \wedge \left(\bigvee_{j \in I_m} \sum_{i \in I_n} t^{u_i} < t^{v_j} \vee \left(\bigwedge_{j \in I_m} \sum_{i \in I_n} t^{u_i} \geq t^{v_j} \wedge \mathcal{B} \right) \right) . \tag{15}$$

Clearly, (15) implies (11). To prove the converse, let $p \geq 2$, $q_i, r_j \geq 0$, with $i \in I_n$ and $j \in I_m$, satisfy (11), i.e. $\sum_{i \in I_n} p^{q_i} < \sum_{j \in I_m} p^{r_j}$. Also, assume that $\sum_{i \in I_n} p^{q_i} \geq p^{r_j}$, for all $j \in I_m$. Then, to prove that (15) is satisfied too by p, q_i, r_j, it is enough to prove that $\mathcal{B}$ is satisfied by p, q_i, r_j. Let p^M be the maximum power of p such that $\sum_{i \in I_n} p^{q_i} \geq p^M$. Since $M \geq q_i$, $i \in I_n$, from Lemma 3.2 it follows that $p^M = \sum_{a \in A} p^{q_a}$, for some $A \subseteq I_n$. Likewise, $M \geq r_j$, $j \in I_m$. But $p^M \leq \sum_{j \in I_m} p^{r_j}$. Thus, again from Lemma 3.2, we have $p^M = \sum_{b \in B} p^{r_b}$, for some $B \subseteq I_m$. Therefore, $\sum_{a \in A} p^{q_a} = \sum_{b \in B} p^{r_b}$, for some $A \subseteq I_n$ and $B \subseteq I_m$, so that, by the same argument used for Case $n > m > 1$ of the reduction of (3), it follows that $\mathcal{B}$ is satisfied by p, q_i, r_j.

As anticipated earlier, we need also to show that the exponentiation operator can be eliminated from atomic formulae of type

$$t^{u_1} = k \tag{16}$$

(with t^{u_1} E-homogeneous) and atoms of type

$$t^{u_1} = t^{v_1} + k \tag{17}$$

(with $t^{u_1} + t^{v_1}$ E-homogeneous), where k is an integer constant.

But this is immediate, since (16) is easily seen to be equivalent to

$$(t \leq 1 \wedge t = k) \vee (t \geq 2 \wedge \bigvee_{\substack{i,j \in I_k \\ i^j = k}} (t = i \wedge u_1 = j)) ,$$

whereas (17) is plainly equivalent to

$$(k = 0 \wedge (t = 0 \vee u_1 = v_1)) \vee (k \geq 1 \wedge \bigvee_{\substack{i,j,\ell \in I_{k+1} \\ i^j = i^\ell + k}} (t = i \wedge u_1 = j \wedge v_1 = \ell)) .$$

Summing up, in view of the decidability of Presburger arithmetic, we have proved

THEOREM 3.3 *The theory* $\mathrm{PAE_{Hom}}$ *is decidable.* □

4 The complexity of unquantified formulae

In this section we sketch the proof that the satisfiability problem for unquantified $\mathrm{PAE_{Hom}}$-formulae is $\mathcal{NP}$-complete.

An inspection of the elimination rules described in the preceding section shows that any given unquantified $\mathrm{PAE_{Hom}}$-formula φ can be transformed into a logically equivalent unquantified formula ψ of PA such that:

(i) the formulae φ and ψ involve the same variables;

(ii) every new integer constant introduced in ψ is $\mathcal{O}(|\varphi|)$, where $|\varphi|$ denotes the length of the formula φ in any convenient encoding.

Thus, it follows from the $\mathcal{NP}$-completeness of linear integer programming (cf. [Pap81,BT76]) that if φ has integer solutions, then it has solutions bounded by $c_\psi^{p(|\psi|)}$, where c_ψ is the maximum constant in ψ and p is a polynomial. Clearly, by (i) and (ii) above, much the same result holds for φ. Specifically, we have that when φ is solvable then it has solutions bounded by $(kc_\varphi)^{p(|\varphi|)}$, where c_φ is the maximum constant in φ, k is an integer constant and p is a polynomial.

To show the $\mathcal{NP}$-completeness of unquantified satisfiable PAE$_{\text{Hom}}$-formulae, it only remains to prove that given q natural numbers $\xi_1, \ldots, \xi_q$ bounded by $(kc_\varphi)^{p(|\varphi|)}$ (one for each free variable x_i occurring in φ), it can be tested in polynomial time whether they constitute a solution of φ. Observe that direct substitution in φ and subsequent numeric computations lead to an at least exponential verification test. Likewise, by using the logically equivalent PA-formula ψ in place of φ, one faces also a running time which is at least exponential, since such is the number of conjuncts of ψ that one may need to verify. For instance, consider the formula

$$\varphi \equiv t \geq 2 \wedge t^{u_1} + t^{u_2} + \ldots + t^{u_n} \neq t^{v_1} + t^{v_2} + \ldots + t^{v_m} \; ,$$

with $n, m \geq 2$. Then φ is equivalent to

$$t \geq 2 \wedge \bigwedge_{\substack{A \subseteq I_n \\ j_0 \in I_m}} \left(\sum_{a \in A} t^{u_a} \neq t^{v_{j_0}} \vee \sum_{i \in I_n \setminus A} t^{u_i} \neq \sum_{\substack{j \in I_m \\ j \neq j_0}} t^{v_j} \right)$$
$$\wedge \bigwedge_{\substack{B \subseteq I_m \\ i_0 \in I_n}} \left(t^{u_{i_0}} \neq \sum_{b \in B} t^{v_b} \vee \sum_{\substack{i \in I_n \\ i \neq i_0}} t^{u_i} \neq \sum_{j \in I_m \setminus B} t^{v_j} \right) .$$

Thus, if $|\varphi|$ is $\mathcal{O}(n)$, then the simple-minded way to certify a purported solution needs to verify the exponentially many conjuncts

$$\sum_{a \in A} t^{u_a} \neq t^{v_{j_0}} \vee \sum_{i \in I_n \setminus A} t^{u_i} \neq \sum_{\substack{j \in I_m \\ j \neq j_0}} t^{v_j} \; ,$$

for each $A \subseteq I_n$, $j_0 \in I_m$.

Alternative transformation rules which solve this problem can be easily devised after the observation that the relation between any two E-homogeneous terms

$$t^{u_1} + t^{u_2} + \ldots + t^{u_n} \quad \text{and} \quad t^{v_1} + t^{v_2} + \ldots + t^{v_m}$$

is completely determined once one knows the relations between the u_i's and the v_j's, and an approximation of the value of t. Specifically, given w_1 and w_2 in $\{u_1, \ldots, u_n, v_1, \ldots, v_m\}$, all the information needed is which of the following relations hold:

$$\begin{array}{lll} w_i & \leq w_{3-i}\,, & i = 1,2 \\ w_i & = w_{3-i} + j\,, & i = 1,2\,, j \leq \max(\lceil \log_2 n \rceil, \lceil \log_2 m \rceil) \\ w_i & > w_{3-i} + \max(\lceil \log_2 n \rceil, \lceil \log_2 m \rceil)\,, & i = 1,2 \\ t & = k & k = 0, 1, \ldots, \max(n,m) \\ t & > \max(n,m)\,. & \end{array} \tag{18}$$

By inductively eliminating exponentiation from the above literals, we finally end up with $\mathcal{O}(|\varphi|)$ exponentiation-free relations of type (18) between the variables occurring in φ. These relations can be used to compute in nondeterministic polynomial time the truth value of any $\mathrm{PAE}_{\mathrm{Hom}}$-formula φ under any given tuple of exponentially bounded numbers.

In a more extended version of this paper we will be more specific on this point and we will explicitly provide such transformation rules.

5 Some applications

Observe that proper E-homogeneous terms are closed under multiplication, in the sense that given any pair of E-homogeneous terms $\{t^{u_1}, t^{u_2}\}$, then the term

$$t^{u_1} \cdot t^{u_2} \equiv t^{u_1+u_2}$$

is also E-homogeneous.

This simple remark allows to conclude that Hilbert's tenth problem becomes solvable when solutions are seeked in certain restricted classes of numbers. Thus, for instance, given a fixed natural number n, by applying the reductions described in Section 3, one can easily decide whether a polynomial Diophantine equation has solutions of the form n^i or whether there exist solution of the form m^i for some m, etc.. This is to be contrasted with the unsolvability of Hilbert's tenth problem in general (cf. [Mat70]).

We also mention that the elimination technique described in the preceding sections can easily be extended to deal also with the array constructs introduced in [SJ80] and with uninterpreted function and predicate symbols (cf. [Sho79]), by suitably redefining E-homogeneous terms and formulae.

6 Open problems

Another way to extend Presburger arithmetic with exponentiation is by allowing exponentiation over a fixed base, i.e. by extending the language of additive arithmetic with terms of the form *exp*$(2,t)$. We conjecture that the resulting fully quantified theory is undecidable, whereas the underlying unquantified theory is decidable.

Acknowledgements

The author wishes to thank V. Cutello and A. Policriti for stimulating conversations.

References

[BFOS81] M. Breban, A. Ferro, E.G. Omodeo, and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. II. Formulas involving restricted quantifiers, together with ordinal, integer, map, and domain notions. *Comm. Pure App. Math.*, XXXIV:177–195, 1981.

[BT76] I. Borosh and L.B. Treybig. Bounds on positive integral solutions to linear Diophantine equations. *Proc. Amer. Math. Soc.*, 55:299–304, 1976.

[CC89] D. Cantone and V. Cutello. *Decision procedures for elementary sublanguages of Set Theory. XVI. Multilevel syllogistic extended by singleton, rank comparison and unary intersection.* Technical Report 439, New York University, Comp. Sci. Dept., April 1989.

[CCP89] D. Cantone, V. Cutello, and A. Policriti. *Set-theoretic reductions of Hilbert's tenth problem.* Technical Report 449, New York University, Comp. Sci. Dept., May 1989.

[CFO] D. Cantone, A. Ferro, and E.G Omodeo. *Computable set theory. Int. Series of Monographs on Computer Science*, Oxford University Press. To appear.

[Chu36] A. Church. A note on the Entscheindungsproblem. *J. Symb. Logic*, 1:40–41, 1936. Correction *ibid.*, 101-102.

[Coo71] D.C. Cooper. Programs for mechanical program verification. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, pages 43–59, American Elsevier, New York, 1971.

[Coo72] D.C. Cooper. Theorem proving without multiplication. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, pages 91–99, American Elsevier, New York, 1972.

[Dav73] M. Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973.

[Dow72] P. Downey. *Undecidability of Presburger arithmetic with a single monadic predicate letter.* Technical Report 18-72, Center for Reasearch in Computing Technology, Harvard University, Cambridge, Mass., 1972.

[End72] H.B. Enderton. *A Mathematical Introduction to Logic.* Academic Press, New York and London, 1972.

[FR74] M.J. Fisher and M.O. Rabin. Super-exponential complexity of Presburger arithmetic. In R.M. Karp, editor, *Complexity of Computation*, 1974. Proceedings of SIAM-AMS Symposium in Applied Mathematics.

[Mat70] Y. Matijasevič. Enumerable sets are Diophantine sets. *Soviet Math. Doklady*, 11:354–357, 1970.

[Opp78] D. Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *J. Comptr. Syst. Sci.*, 16(3):323–332, 1978.

[Pap81] C.H. Papadimitriou. On the complexity of integer programming. *J. A.C.M.*, 28(4):765–768, 1981.

[PP88] F. Parlamento and A. Policriti. Decision procedures for elementary sublanguages of set theory. IX. Unsolvability of the decision problem for a restricted subclass of the Δ_0-formulas in set theory. *Comm. Pure App. Math.*, XLI:221–251, 1988.

[Pre29] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetic ganzer Zahlen, in welchem die addition als einzige Operation hervortritt. In *Comptes-rendus du Premier Congrès des Mathematiciens des Pays Slaves*, pages 192–201, Warsaw, 1929.

[RD78] C.R. Reddy and Loveland D.W. Presburger arithmetic with bounded quantifier alternation. In *Proc. Tenth Annual ACM Symposium on the Theory of Computing*, pages 320–325, 1978.

[Sca84] B. Scarpellini. Complexity of subcases of Presburger arithmetic. *Trans. Amer. Math. Soc.*, 284(1):203–218, 1984.

[Sho79] R.E. Shostak. A practical decision procedure for arithmetic with function symbols. *J. A.C.M.*, 26(2):351–360, 1979.

[SJ80] N. Suzuki and D. Jefferson. Verification decidability of Presburger array programs. *J. A.C.M.*, 27(1):191–205, 1980.

NYU COMPSCI TR-450
Cantone, D
On the decidability of
Presburger arithmetic with
homogeneous... c.1

DATE DUE	BORROWER'S NAME

TR-450